UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

MICHELLE BIRNIE, CHAROLET WADEINE FAIL, AND LAUREN WILKINSON, on behalf of themselves and all others similarly situated, Plaintiffs, v. **CITRIX SYSTEMS, INC.,** a Delaware Corporation, Defendant.	**Case No. 24-1201** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs Michelle Birnie, Charolet Wadeine Fail, and Lauren Wilkinson ("Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following based upon their personal knowledge as to the allegations regarding themselves, and as to all other allegations, based on the investigation of their counsel and information and belief:

INTRODUCTION

1. Plaintiffs bring this class action against Citrix Systems, Inc. ("Citrix") on behalf of themselves and all others similarly situated who were harmed by a data breach announced by Xfinity in December 2023 that compromised the personal information of more than 35 million customers (the "Data Breach"). The Data Breach was the direct result of a security vulnerability in a Citrix product called the Citrix NetScaler Application Delivery Controller and NetScaler Gateway that is used by Xfinity and thousands of other organizations. The Citrix NetScaler

Application Delivery Controller and NetScaler Gateway product allows organizations to enable secure remote access and optimize, manage, and secure network traffic.

2. Citrix is a global cloud computing and software company. It provides its customers with technology that allows for a secure digital workspace. The company also provides "networking solutions" that deliver applications and data that its customers' employees need to be productive. Citrix serves more than 100 million users across 100 countries.

3. The security vulnerability—dubbed “Citrix Bleed”—is particularly dangerous because it allows unauthorized third parties to bypass multifactor authentication and essentially hijack legitimate user sessions and acquire elevated permissions to harvest credentials, move laterally within the subject network, and access data and resources.

4. Citrix announced the security vulnerability on October 10, 2023, and issued a patch. On October 25, 2023, however, Citrix issued additional mitigation guidance. Xfinity says it promptly installed the patch and mitigated its systems. During its investigation, however, Xfinity discovered that between October 16 and October 19, the security vulnerabilities allowed hackers to access Xfinity’s internal systems and steal the personal identifying information belonging to over 35 million Xfinity customers.

5. Hackers, exploiting Citrix Bleed, were able to steel a treasure trove of customer information from Xfinity, including usernames and hashed passwords, names, contact information, the last four digits of Social Security numbers, dates of birth, and security questions and answers (“Personal Identifying Information” or “PII”). Recent reports indicate that the PII of over 35 million Xfinity customers was stolen. Xfinity informed customers of the Data Breach in December 2023. The PII that was stolen from Xfinity, either alone or in combination with other personal

identifying information that might be available on the dark web, can be used by identity thieves to commit a wide range of identity theft.

6. Xfinity is not the only Citrix customer negatively impacted by Citrix Bleed. In November 2023, reports indicate that Russian-based ransomware group LockBit 3.0 was able to exploit Citrix Bleed to attack Boeing, even after Citrix had issued the patch and mitigation guidance. Other organizations reportedly affected by Citrix Bleed include the International Commerce Bank of China, the logistics company DP World, and the law firm of Allen & Overy, among others.

7. The Data Breach resulted from Citrix's sale of the Citrix NetScaler Application Delivery Controller and NetScaler Gateway with security vulnerabilities and because of its numerous failures, including failing to adequately test and monitor its products for security vulnerabilities, failing to identify the security vulnerabilities earlier, and failing to adequately and promptly notify its customers of the security vulnerabilities. This is not the first time that Citrix's conduct and omissions have compromised sensitive and personal identifying information. In 2019, Citrix suffered two other security incidents that compromised personal identifying information of thousands of persons.

8. As a result of the Data Breach, Plaintiffs' and Class members' PII has been exposed to criminals for misuse. The injuries Plaintiffs and the Class have suffered, and will continue to suffer, include: identity theft; financial losses caused by misuse of their PII; the loss in value of their PII as a result of the Data Breach; lost time and costs associated with the detection and prevention of identity theft; and lost time and costs associated with spending time to address and mitigate the actual and future consequences of the breach.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 proposed class members.

10. This Court has personal jurisdiction over Citrix because Citrix has committed acts within the Eastern District of Pennsylvania giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Citrix would not offend traditional notions of fair play and substantial justice. Citrix has engaged in continuous, systematic, and substantial activities within this State, including substantial marketing and sales of services and products—including Citrix's NetScaler software used by Xfinity in connection with the Data Breach—within this state.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, Citrix maintains its headquarters within this District, and Citrix caused harm to Class members residing in this District.

PARTIES

12. Plaintiff Michelle Birnie is a resident and citizen of Key Largo, Florida. On December 30, 2023, Ms. Birnie received a text message from Xfinity telling her to change her password. Later, on January 4, 2024, Ms. Birnie received a letter via email from Xfinity informing her that her personal information was compromised. Since December 19, 2023, Ms. Bernie has experienced identity theft as alleged herein.

13. Plaintiff Charolet Wadeine Fail is a resident and citizen of Sebring, Florida. On January 3, 2024, Ms. Fail received a letter in the mail from Xfinity informing her that her personal information was compromised. Since November 2023, Ms. Fail has experience identity theft as alleged herein.

14. Plaintiff Lauren Wilkinson is a resident and citizen of Reading, Pennsylvania. On January 4, 2024, when Ms. Wilkinson logged into her Xfinity account, she received notice from Xfinity informing her that her personal information was compromised. As a result of the Data Brach, Ms. Wilkinson has spent time and effort, and continues to spend time and effort, monitoring her financial accounts and online accounts to detect and prevent any fraudulent or suspicious activity.

15. Defendant Citrix Systems, Inc. is a Delaware corporation with its principal place of business in Fort Lauderdale, Florida.

FACTUAL ALLEGATIONS

A. Background on Citrix

16. Citrix is a cloud computing and virtualization technology company. It designs, develops, and sells software that allows for a digital workspace. Its "digital workspace [] provides unified, secure, and reliable access to all applications and content employees need to be productive – anytime, anywhere, on any device."[1]

17. Citrix has customers and offices throughout the world. It serves "more than 100 million users, 10,000 partners and 400,000 customers across 100 countries."[2] As of early 2021, the company had over 10,000 employees in more than 40 countries.[3]

[1] https://www.citrix.com/about/sustainability/2020-report/data-index.html#:~:text=Citrix%20serves%20more%20than%20100,400%2C000%20customers%20across%20100%20countries.
[2] *Id.*
[3] *Id.*

18. The company markets its solutions and services as designed "to deliver applications and data with the security and controls necessary to protect the enterprise and its customers."[4]

B. Citrix knew about its cybersecurity vulnerabilities.

19. As a cloud computing company, Citrix is well aware of the risks associated with failing to adequately protect against security vulnerabilities. In past public filings, Citrix acknowledged that "service vulnerabilities could result in loss of and/or unauthorized access to confidential information."[5]

20. Citrix also conceded that it had "in the past, and may in the future, discover[ed] vulnerabilities in [its] products or underlying technology, which could expose . . . customers to risk."[6]

21. For example, in March 2019, Citrix disclosed that hackers had gained access to its networks. For more than four months, the hackers had exploited vulnerabilities in Citrix's networks and stole names, Social Security numbers, and financial information relating to Citrix's current and former employees, as well as some beneficiaries and dependents of those employees.

22. That March 2019 data breach was the subject of a class action lawsuit against Citrix in this District, *In re: Citrix Data Breach Litigation,* Case No. 19-cv-61350-RKA. The case settled in 2021. As part of that settlement, in addition to providing monetary compensation to individuals affected by the breach, Citrix agreed to certain business practice commitments and remedial measures concerning data security for at least three years. Those commitments included: (1) enhanced cybersecurity training and awareness programs; (2) enhanced data security policies; (3)

---

[4] *Id.*
[5] Citrix Systems, Inc. Form 10-K for the fiscal year ending on December 21, 2021 (https://www.sec.gov/ix?doc=/Archives/edgar/data/0000877890/000087789022000019/ctxs-20211231.htm).
[6] *Id*.

enhanced security measures; (4) further restricting access to personal information; and (5) enhanced monitoring and response capability. *See In re: Citrix Data Breach Litig.,* Case No. 19-cv-61350-RKA, Dkt. 64 at 9.

23. Yet in December 2019, the company discovered another vulnerability in some of its "Application Delivery and Security products that would have allowed an unauthenticated attacker to perform arbitrary code execution."[7] Citrix reported that its response to this vulnerability "required significant investment of resources across the company."[8]

C. Citrix Bleed

24. On October 10, 2023, Citrix disclosed multiple security vulnerabilities in its NetScaler Application Delivery Controller ("ADC") and NetScaler Gateway products. An ADC is a hardware device or software program that manages the flow of traffic between users of a website and the website's servers with the goal of optimizing the experience of end users. NetScaler Gateway provides remote access infrastructure, including virtual servers, authentication and authorization of user access, user connection methods, and additional network resources. In other words, NetScaler Gateway allows an entity to securely manage remote access to its networks. Seventy-five percent of internet users rely on NetScaler every day, and 90% of the Fortune 500 rely on NetScaler.

25. Citrix, however, described the vulnerabilities (identified as CVE-2023-4966 and CVE-2023-4967) only as "unauthenticated buffer-related" issues.

26. The Citrix security vulnerabilities, dubbed "Citrix Bleed," have been connected to several cyberattacks, including against Boeing and Toyota. Citrix Bleed affects several versions of the

[7] *Id.*
[8] *Id.*

NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) products.

27. The vulnerabilities are said to be easy to exploit. While Citrix also issued a purported fix on October 10, 2023, in connection with its disclosure, it did not issue mitigation guidance warning its customers to download the patches immediately until October 23, 2023. Despite the fix, mitigation guidance, and installation of the patches, hackers have been nevertheless able to attack numerous organizations.

28. Charles Carmakal, CTO at Mandiant Consulting, Google Cloud, reported, "We observed hijacking at organizations who updated their Netscaler devices." Mandiant has warned users to "terminate all active or persistent sessions to prevent further attacks." Mandiant also reported that before October 10, it had been investigating cases where threat actors were taking over Netscaler sessions though an "unknown means." Other reports indicate that Citrix Bleed has been exploited in the wild since August 2023, which the Cybersecurity and Infrastructure Security Agency ("CISA") has confirmed.

29. According to a cybersecurity advisory issued by CISA, which reviewed data voluntarily shared by Boeing, "Citrix Bleed, known to be leveraged by LockBit 3.0 affiliates, allows threat actors to bypass password requirements and multifactor authentication (MFA), leading to a successful hijacking of legitimate user sessions on Citrix NetScaler web application delivery control (ADC) and Gateway appliances."

30. Josh Amishav, CEO of the cybersecurity firm Breachsense, said that "Citrix Bleed is dangerous because it allows malicious users to access sensitive data coupled with the fact that it affects commonly used Citrix devices in large organizations . . . This means that the vulnerability can be exploited en masse, leading to significant data breaches."

D. Citrix Bleed results in unauthorized access to Xfinity customers' personal identifying information

31. Citrix Bleed has provided hackers with unauthorized access to stored data belonging to several Citrix customers, including Xfinity customer data. Before Citrix issued its mitigation guidance, between October 16 and October 19, 2023, hackers gained unfettered access to Xfinity's systems by exploiting Citrix Bleed.

32. In December 2023, Xfinity announced that hackers had stolen the PII of more than 35 million Xfinity customers, including names, contact information, last four digits of Social Security numbers, dates of birth, secret questions and answers, and usernames and passwords.

33. Xfinity notified all its customers of the security incident and asked them to change their passwords. Xfinity also encouraged its customers to enroll in multi-factor authentication, advised them not to re-use passwords across multiple accounts, and if they had re-used passwords elsewhere, to also change the passwords of those accounts.

E. The data breach was avoidable and foreseeable.

34. Citrix could have prevented the Xfinity data breach by developing and selling secure hardware and software, conducting ongoing testing of its products for security vulnerabilities, taking adequate and reasonable measures to monitor its software for security vulnerabilities, and taking adequate and prompt measures to develop an adequate response and issue effective notice to its customers. As alleged herein, Citrix Bleed has likely been exploited in the wild since August 2023, and since before the Citrix announcement on October 10, 2023, Mandiant had investigated the hijacking of Netscaler sessions via unknown means that were subsequently revealed to be as a result of Citrix Bleed.

35. Citrix was well aware of the need to protect the PII that its customers maintain using its networks and products. The PII compromised in the Data Breach is a valuable commodity to

identity thieves, and Citrix knew of the likelihood of attempted cyberattacks. In fact, Citrix's public filings and history of security vulnerabilities make clear that Citrix realized the risks of unsecured products.

36. The Federal Trade Commission has established guidelines for fundamental data security principles and practices for businesses.[9] Among other things, the guidelines note businesses should understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to discover a security vulnerability as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, and have a response plan ready in the event of a breach.[10]

37. Citrix was at all times aware of its obligations under federal and state laws and regulations to protect its customers' data. Despite that awareness, Citrix fell short of satisfying its legal obligations. Among other things, Citrix failed to implement and maintain reasonable measures to address security vulnerabilities.

F. The data breach harmed Plaintiff and Class members and will cause additional harm.

38. Individuals who have been victims of data breaches are much more likely to become victims of identity theft than those who have not. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9).

[9] Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[10] *Id*.

39. PII is highly valuable to identity thieves because, as the FTC explains, "[o]nce identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[11]

40. The information compromised in this Data Breach is more valuable than the loss of, for example, credit card information in a retailer data breach. With retailer data breaches, victims can close credit and debit card accounts, typically for free. Here, the information compromised—Social Security numbers, names, contact information, and dates of birth—are not like accounts that can be closed—rather, they are difficult, if not impossible, to change.

41. As a direct and proximate result of Citrix's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs and Class members' PII, Plaintiffs and Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other injuries, including:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

b. Lost value of their PII as a result of its theft and unauthorized use;

c. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

d. Lost opportunity costs and lost wages associated with expended efforts and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; and

[11] http://www.leginfo.ca.gov/pub/15-16/bill/asm/ab_1551
1600/ab_1580_cfa_20160613_144620_sen_comm.html

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of Plaintiffs' and Class members' lives.

42. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

43. To date, other than Xfinity asking Class members to reset their passwords, Plaintiffs and Class members have not received any assistance in dealing with the theft of their PII.

PLAINTIFFS' EXPERIENCES

Ms. Michelle Birnie

44. Ms. Birnie has been a victim of several identify theft incidents since December 19, 2023. An unauthorized person(s) attempted to purchase flights from Kuala Lumpur for $432.00 on three different booking websites using her debit card information. Ms. Birnie had to spend time resolving the issue, including canceling and changing her debit card. While she was on the phone with her bank, she received numerous login attempt notifications for her Amazon account about every two minutes. As a result of these hacking attempts, Ms. Birnie had to change all of her passwords, including her Xfinity, Amazon, and financial accounts.

45. As a result of the Data Breach, Ms. Birnie has spent time and effort, and continues to spend time and effort, researching and monitoring her financial and online accounts in an effort to detect and prevent any further misuse. Ms. Birnie has also lost time from work.

Ms. Charlotte Wadeine Fail

46. Beginning in November 2023 and continuing through the first week of January 2024, over

a dozen unauthorized charges were made against Ms. Fail's checking account. The charges were not flagged by her bank because they appeared as Xfinity charges. Ms. Fail was able to get all of the charges reversed except for two in the amounts of $154.73 and $277.22. The unauthorized charges, however, triggered 15 overdraft charges for $30 each totaling $450.00, which Ms. Fail is now responsible. Ms. Fail is currently working with her bank to resolve the unauthorized charges, including the overdraft charges.

47. Ms. Fail has made countless trips back and forth between her bank and the local Xfinity store dealing with the unauthorized charges, the overdraft charges, getting a replacement debit card, and eventually closing her checking account. Within a week of closing her checking account and opening a new one, her checking account balance went from $300 to $2.

48. The fraudulent charges also affected her electronic automatic payments, including to her auto insurance and cell phone carrier. Ms. Fail had to contact every company with which she has automatic withdrawal set up to explain that she has been a victim of identity theft and to stop the withdrawals. She also had to contact the Social Security Administration to make sure her Social Security checks were not compromised and to ensure her checks were deposited.

49. As a result of the Data Breach, Ms. Fail has spent time and effort, and continues to spend time and effort, changing all of her passwords for her Xfinity and financial accounts, researching and monitoring her financial and online accounts in an effort to detect and prevent any further misuse, including setting up monitoring through her bank.

Ms. Lauren Wilkinson

50. On January 4, 2024, when Ms. Wilkinson logged into her Xfinity account, she received notice from Xfinity informing her that her personal information was compromised in the Data Breach. As a result of the Data Brach, Ms. Wilkinson has spent time and effort, and continues to

spend time and effort, monitoring her financial accounts and online accounts to detect and prevent any fraudulent or suspicious activity.

CLASS ALLEGATIONS

51. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of the following nationwide class ("Nationwide Class"):

> All persons in the United States whose personal information was compromised in the data breach publicly announced by Xfinity in December 2023.

52. Excluded from the proposed Class are Defendant Citrix Systems, Inc., including any entity in which Citrix has a controlling interest, is a subsidiary, or which is controlled by Citrix, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Citrix.

53. Plaintiffs reserve the right to amend or modify the class definition with greater specificity or division, or create and seek certification of additional classes, after having had an opportunity to conduct discovery.

54. Numerosity: The Class members are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Reports indicate that over 35 million individuals were affected by the Data Breach.

55. Commonality and Predominance: Common questions of law and fact exist as to the proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Citrix knew or should have known that its products were vulnerable to unauthorized access;

b. Whether Citrix failed to take adequate and reasonable measures to monitor security vulnerabilities in its products;

c. Whether Citrix failed to take available steps to prevent and stop the breach from happening;

d. Whether Citrix owed a legal duty to Plaintiffs and Class members to protect their PII;

e. Whether Citrix breached the duty to Plaintiffs and Class members by failing to exercise due care in protecting their PII;

f. Whether Plaintiffs and Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

g. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief or restitution.

56. **Typicality:** Plaintiffs' claims are typical of the claims of other Class members. All Class members were subject to the Data Breach that resulted from Citrix Bleed and had their PII accessed by and/or disclosed to unauthorized third parties.

57. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in class action litigation and data breach litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

58. **Declaratory and Injunctive Relief:** The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Citrix. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Citrix has acted and/or refused to act on grounds

generally applicable to the Class, making injunctive relief or corresponding declaratory relief appropriate.

59. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Citrix, making it impracticable for Class members to individually seek redress for Citrix's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individual litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE

60. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

61. Citrix negligently sold products that were vulnerable to exploitation and that were inadequate to safeguard access to its customers' networks and data. Citrix did so despite marketing its NetScaler products as providing comprehensive security and allowing businesses to manage VPN connectivity and application delivery. As a result of the vulnerabilities in Citrix's products, attackers could gain access to sensitive information, including PII belonging to Plaintiffs and Class members.

62. It was reasonably foreseeable to Citrix that its failure to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of its NetScaler products could subject its customers to breach of sensitive information and could thus expose the owners of that information to harm.

63. Citrix owed a duty to Plaintiffs and Class members to ensure that its products—and the personnel responsible for them—adequately protected their personal identifying information.

64. Citrix's duty of care arose as a result of Citrix's knowledge that customers trusted its products to provide secure access to the customers' own networks and applications. Citrix advertised its products as providing "comprehensive security for all applications" and "secure remote access solution[s]."

65. Only Citrix was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and Class members as a result of the Data Breach, which exploited vulnerabilities in Citrix's products. It was foreseeable that Plaintiffs and Class members would be the victims of Citrix's inadequate data security practices: Citrix knew that it was more likely than not that Plaintiffs and Class members would be harmed in the event of a data breach.

66. In addition, Citrix had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

67. Citrix also had a duty to use reasonable care in protecting confidential data because it committed to complying with industry standards for the protection of personal information.

68. Citrix knew, or should have known, of the risks inherent in the vulnerabilities in its NetScaler products, and the importance of adequate security to NetScaler users.

69. By failing to use reasonable measures to secure its NetScaler product, Citrix breached its duties to Plaintiffs and Class members.

70. Plaintiffs and Class members have suffered harm as a result of Citrix's negligence. Such harms include the following: ongoing, imminent, impeding threat of identity theft and fraud, resulting in monetary loss, economic harm, and loss of time; actual identity theft and fraud, resulting in monetary loss, economic harm, and loss of time; loss of value in their PII; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the data breach reviewing bank statements, credit card statements, and credit reports, among other activities; and expenses and time spent initiating fraud alerts.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*

71. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

72. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Citrix, of failing to use reasonable measures to protect personal information. 15 U.S.C. § 45(a)(1).

73. The FTC publications and orders described above also form part of the basis of Citrix's duty in this regard.

74. Citrix violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and not complying with applicable industry standards, as described herein. Citrix's conduct was particularly unreasonable given the nature and amount of personal information that its customers obtain and store, and the foreseeable consequences of security vulnerabilities in Citrix's products that could lead to hackers stealing that information.

75. Citrix's violation of Section 5 of the FTC Act constitutes negligence per se.

76. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

77. The harm that occurred as a result of the Data Breach (and the security vulnerability that led to the breach) is the type of harm that the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm as that suffered by Plaintiffs and the Class.

78. Moreover, Florida law requires that covered entities "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. § 501.171(2).

79. "Covered entity" includes any "commercial entity that acquires, maintains, stores, or uses personal information." Fla. Stat. § 501.171(1)(b).

80. "Personal information" means "[a]n individual's first name or first initial and last name in combination with" several additional data elements for that individual, including Social Security number; driver's license or identification card number; and/or financial account number or credit or debit card number. Fla. Stat. § 501.171(1)(g).

81. Citrix violated § 501.171(2) by failing to take reasonable measures to protect and secure Plaintiffs' and Class members' personal information.

82. The harm that occurred as a result of the Data Breach is the type of harm section 501.171(2) was intended to guard against, and Plaintiffs and the Class are in the class of persons the section was intended to protect.

83. Citrix's violation of § 501.171(2) constitutes negligence per se.

84. As a direct and proximate result of Citrix's negligence per se, Plaintiffs and Class members have suffered and will suffer injury and damages, including but not limited to: (i) the loss of the

opportunity to determine for themselves how their personal information is used; (ii) the publication and/or theft of their personal information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their personal information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII; and, (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the consequences of compromised personal information for the rest of their lives.

THIRD CAUSE OF ACTION
VIOLATIONS OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq.*

85. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

86. Citrix engaged in the conduct alleged in this complaint through transactions in and involving trade and commerce. The security vulnerabilities at issue occurred through the internet, an instrumentality of interstate commerce.

87. Citrix engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following:

a. Developing and selling products and networks with security vulnerabilities;

b. Failure to test and monitor its products and networks for securities vulnerabilities to safeguard its customers' data;

c. Failure to implement adequate data security practices on its products and networks to safeguard its customers' data;

d. Failure to disclose that its products, networks, and data security practices were inadequate to safeguard personal information from theft;

e. Failure to adequately and promptly notify customers of the security vulnerabilities in its products and networks; and

f. Failure to timely mitigate the security vulnerabilities that caused the Data Breach.

88. Citrix's actions are unconscionable, deceptive, or unfair acts or practices because Citrix engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Plaintiffs and Class members.

89. In committing the acts alleged above, Citrix engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to its customers that it did not follow industry best practices for securing its networks.

90. As a direct and proximate result of Citrix's conduct, Plaintiffs and Class members have been harmed and have suffered damages, including: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

91. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs and Class members have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorney's fees and costs.

92. Also, as a direct result of Citrix's violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Citrix engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Citrix's systems on a periodic basis, and ordering Citrix to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Citrix engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Citrix audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Citrix conduct regular database scanning and securing checks;

e. Ordering that Citrix segment information by, among other things, creating firewalls and access controls so that if one area of Citrix is compromised, hackers cannot gain access to other portions of Citrix's systems.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of all others similarly situated, respectfully request the following relief:

f. An order certifying the proposed Class, appointing Plaintiffs as class representatives and their undersigned counsel as class counsel;

g. An order finding that Citrix engaged in the unlawful conduct as alleged herein;

h. An order enjoining Citrix from engaging in the wrongful conduct alleged herein;

i. A mandatory injunction directing Citrix to adequately safeguard its networks and Plaintiffs' and Class members' PII by implementing improved security procedures and measures;

j. An award of compensatory, statutory, and punitive damages, as appropriate, in an amount to be determined;

k. An award of pre-judgment and post-judgment interest on all amounts awarded;

l. An award of Plaintiffs' and Class members' reasonable attorney's fees and litigation expenses; and

m. Such other relief as the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial on all issues so triable.

Dated: March 20, 2024

LEVIN SEDRAN & BERMAN LLP

By: /s/ *Charles E. Schaffer*
Charles E. Schaffer
Nicholas J. Elia
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Email: cschaffer@lfsblaw.com
Email: nelia@lfsblaw.com

Rosemary M. Rivas (*pro hac vice* forthcoming)
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9700
Facsimile: (510) 350-9701
Email: rmr@classlawgroup.com

Attorneys for Plaintiffs and the Proposed Class Members